UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

ECOLAB Inc., and NALCO COMPANY LLC d/b/a Nalco Water, an Ecolab Company and/or Nalco Water, Plaintiffs, v. JESSICA GRAILER, Defendant.	Case No.: 3:23-cv-00102-wmc

DECLARATION OF BRUCE W. PIXLEY

I, Bruce W. Pixley, declare under penalty of perjury that the following is true and correct:

I. Background

1. I am the Managing Member of Pixley Forensics Group LLC. My responsibilities include assisting corporate clients and law firms in investigations and disputes involving forensic accounting issues, electronic discovery, theft of intellectual property, and computer forensic investigations. In this capacity, I manage teams of forensic examiners and use a variety of technologies to perform data acquisition and analysis of this information.

2. Starting in 2001, I served as a lead instructor of computer forensics, Internet investigations, and network intrusion courses for the California Department of Justice's Advanced Training Center. Additionally, I have been employed as a Master Instructor at Guidance Software, which developed the EnCase computer forensic software. As an instructor, I have taught for over 2,000 hours on the subjects of computer forensics and high-tech investigations. I have developed course training materials and wrote manuals for computer forensic courses such as Advanced Internet Examinations and Network Intrusion Investigations.

3. I possess three professional certifications for my fields of work. I possess the Certified Information Systems Security Professional (CISSP) certification and the GIAC Certified Forensic Analyst (GCFA) certification, which are both ANSI ISO accredited credentials, and the EnCase Certified Examiner certification.

4. Since 2003, I have been retained as a computer forensic examiner and subject matter expert in both criminal and civil matters. I have been qualified as an expert witness in both state and federal courts and testified about the foundation of computer forensics, Windows and Mac operating systems, chat software, Internet and network operations, e-mail, peer-to-peer file sharing, digital photography, recovery of deleted data, and Trojan viruses.

5. Attached as **Exhibit A** to this declaration is a copy of my current Curriculum Vitae, which sets forth in detail additional aspects of my qualifications and background.

6. I have been retained by Quarles & Brady LLP, counsel for Defendant Jessica Grailer, to provide technical computer forensic services.

II. Background on Microsoft Audit Logs and Their Importance

7. Traditionally, Microsoft servers have created various types of audit logs used for investigation. Microsoft 365 is a cloud-based service that employs audit logging to detect activities and capture details about system configuration changes and access events. A Microsoft audit log is automatically generated and identifies the user or system responsible for different activities, when and where the activities took place, and the outcome of the activities. Just like other digital evidence that is preserved for a civil or criminal matter, a complete audit log is treated as evidence.

8. When Microsoft provides cloud services to customers, such as OneDrive for files and Exchange for email, Microsoft creates audit logs that can be used for investigation and evidentiary purposes. The Microsoft audit logs available today are far more robust with

information than they were in the past.

9. A Microsoft audit log provides detailed, granular information regarding events involving both system-level functions and user-related functions, such as if a person accesses, moves, copies, deletes, or downloads a file. Each event record in the audit log may contain more than 40 different fields of relevant information. The Microsoft Purview website portal under Microsoft Learn, one printout from which is attached as **Exhibit B**, explains how a Microsoft audit log can be exported, configured, and viewed. An exported audit log includes various fields of information, including but not limited to "RecordID," "CreationDate," "Operation," "UserId," "AppAccess," "CreationTime," "Id," Operation.1," "OrganizationId," "RecordType.1," "UserKey," "UserType," "Version," "Workload," "ClientIp," "ObjectId," "AuthenticationType," "BrowserName," "BrowserVersion," "CorrelationId," "EventSource," "IsManagedDecive," "ItemType" "ListId, and "ListItemUniqueId."

10. Attached to this declaration as **Exhibit C** are screenshots of a sample Microsoft audit log export, to illustrate the robust data that such a log contains.

11. In my years of investigating activity involving Microsoft cloud services, I have found it absolutely necessary to obtain complete audit logs from customers' Microsoft accounts. A Microsoft audit log provides a complete timeline of events and is a critical piece of digital evidence. Such an audit log is readily available, easily accessed, and will assist in determining what a person may or may not have done. Audit log data covering even long periods of time and large volumes of activity can be exported conveniently as a single .csv or Excel file. As described above, Microsoft provides instructions on its website describing how to access, search, export, and format an audit log (*see, e.g.,* **Ex. B**).

12. In a declaration filed in this case, Laurence D. Lieb alleges that Defendant accessed

her work-issued OneDrive account on January 14, 2023, and additionally that on January 15, 2023, she accessed her OneDrive account and "exfiltrated" twenty files. (Dkt. 15, ¶¶ 16–17.) Plaintiffs' Microsoft audit log would include data recording those specific activities, if they in fact occurred.

13. Obtaining a complete (not partial) audit log is necessary, as it is important for someone who is reviewing the audit log to be objective by reviewing all of the details in each record, along with all of the surrounding events and details.

14. During my collection of a Microsoft audit log, I would document the process that I used to search and export the audit log as evidence. This documentation would allow me to authenticate this digital evidence so it could be introduced in a court proceeding in the future.

III. The Spreadsheet Plaintiffs Produced is Not a Microsoft Audit Log

15. I have received and reviewed a copy of an Excel spreadsheet (JGrailer.xlsx) that was sent by Plaintiffs' counsel, James Hux, via email to Defendant's counsel on May 3, 2023. The email message from Attorney Hux indicated that the Excel spreadsheet was "a report that relates to One Drive Access." In some of its rows, the spreadsheet references the same 20 files that Laurence Lieb lists in paragraph 17 of his declaration (Dkt. 15, ¶ 17, Table A.)

16. The JGrailer.xlsx spreadsheet that Plaintiffs provided is not a Microsoft audit log. It provides only six fields of information for each record, as opposed to the over 40 fields of information that would be in a Microsoft audit log. In addition, the field names used at the top of each column in Plaintiffs' spreadsheet (@timestamp, event.action, event.outcome, source.ip, file.name, and user_agent.original) do not appear in an actual Microsoft audit log. Further, the spreadsheet lists events, such as "FilePreviewed" events, that should be associated with a username and be adjacent to other preceding or following events if they reflected user-related activity—but in Plaintiffs' spreadsheet neither of those things is true. The spreadsheet is not a Microsoft audit

log and appears to be fragments of information that an unknown person assembled from an unknown source.

Executed on this 9th day of August 2023.

Bruce W. Pixley